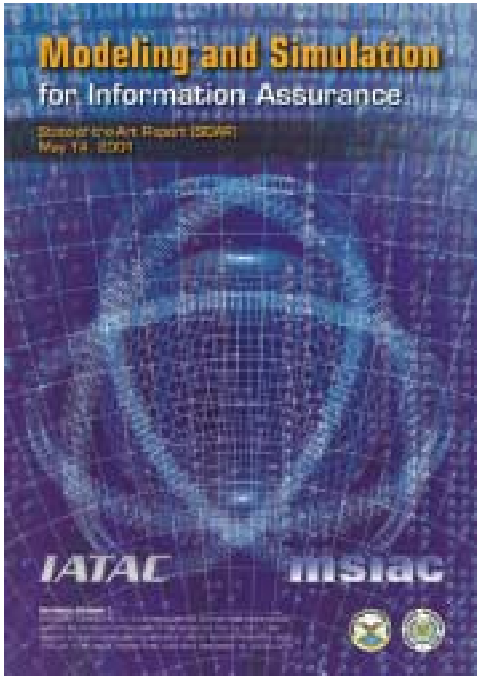
Modeling & Simulation for Information Assurance State-of-the-Art Report (SOAR)

A Summary


Modeling and Simulation
for Information Assurance
State-of-the-Art Report (SOAR)
May 14, 2001
IATAC msiac

Principal Author: Gary L. Waag, *IATAC*
R. Kenneth Heist, *MSIAC*
Dr. Jerry M. Feinberg, *MSIAC*
Lesley J. Painchaud, *MSIAC*

msiac
MODELING AND SIMULATION
INFORMATION ANALYSIS CENTER

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 1/1/2000	**3. REPORT TYPE AND DATES COVERED** Report 1/1/2000

4. TITLE AND SUBTITLE Modeling & Simulation for Information Assurance State- of-the- Art Report (SOAR)	**5. FUNDING NUMBERS**
6. AUTHOR(S) R. Kenneth Heist, Dr. Jerry M. Feinberg, Lesley J. Painchaud, Gary L. Waag	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) IATAC MSIAC 3190 Fairview Park Drive Falls Church, VA 22042	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT *(Maximum 200 Words)*

Provides a sumary of the Modeling & Simulation for Information Assurance State-of-the-Art Report (SOAR) created by IATAC and MSIAC.

14. SUBJECT TERMS IATAC Collection, information assurance, information operations	**15. NUMBER OF PAGES** 27
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** abstract_limitation

Purpose of Briefing

- Provide an overview of the objectives, findings and recommendations of the …
  - Information Assurance Modeling & Simulation (IA M&S) State-of-the-Art Report (SOAR)
    - A report jointly sponsored by the Defense Technical Information Center (DTIC's) …
      - Information Assurance Technology Analysis Center (IATAC)
      - Modeling and Simulation Information Analysis Center (MSIAC)

Outline

- Background
- Types of IA M&S
- Summary, Conclusions, Needs

Definitions

- Information Operations (IO)
  - “Those actions taken to affect an adversary's information and information systems while defending one's own information and information systems.” [1]
- Information Assurance (IA)
  - "Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." [2]

[1] "National Information Systems Security (INFOSEC) Glossary," NSTISSI No. 4009, January 1999.

[2] "U.S. Joint Vision 2020", OPR Director for Strategic Plans and Policy, J5, Strategic Division, available at: http://www.dtic.mil/jv2020/jvpub2.htm

Objective of SOAR

- To develop an assessment of the current state-of-the-art of modeling and simulation (M&S) to support Information Assurance (IA)
- Collect information that describes:
  - tools
  - data
  - and other research activities

Target Audience & Benefits

- Primary audience of this assessment is the IA community within the U.S. Department of Defense (DoD)
  - those people and organizations directly responsible for the protection and defense of information and information systems.
- Benefits:
  - help leverage existing knowledge and capabilities while avoiding unnecessary duplication of effort, in turn, helping to foster reuse and interoperability of such tools.

Approach

1. Determine what we want to Survey

- Develop Taxonomy

2. Determine how to get it

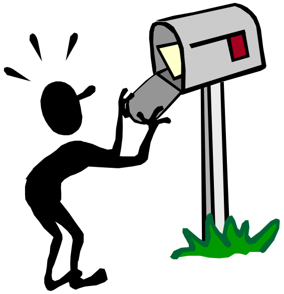
- Create Questionnaire
- Identify IO/IA focused orgs & POCs

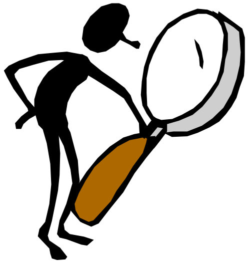
3. Go get it

- Circulate survey to individuals
- Broadcast survey to groups of potential interest
- Conduct open literature search

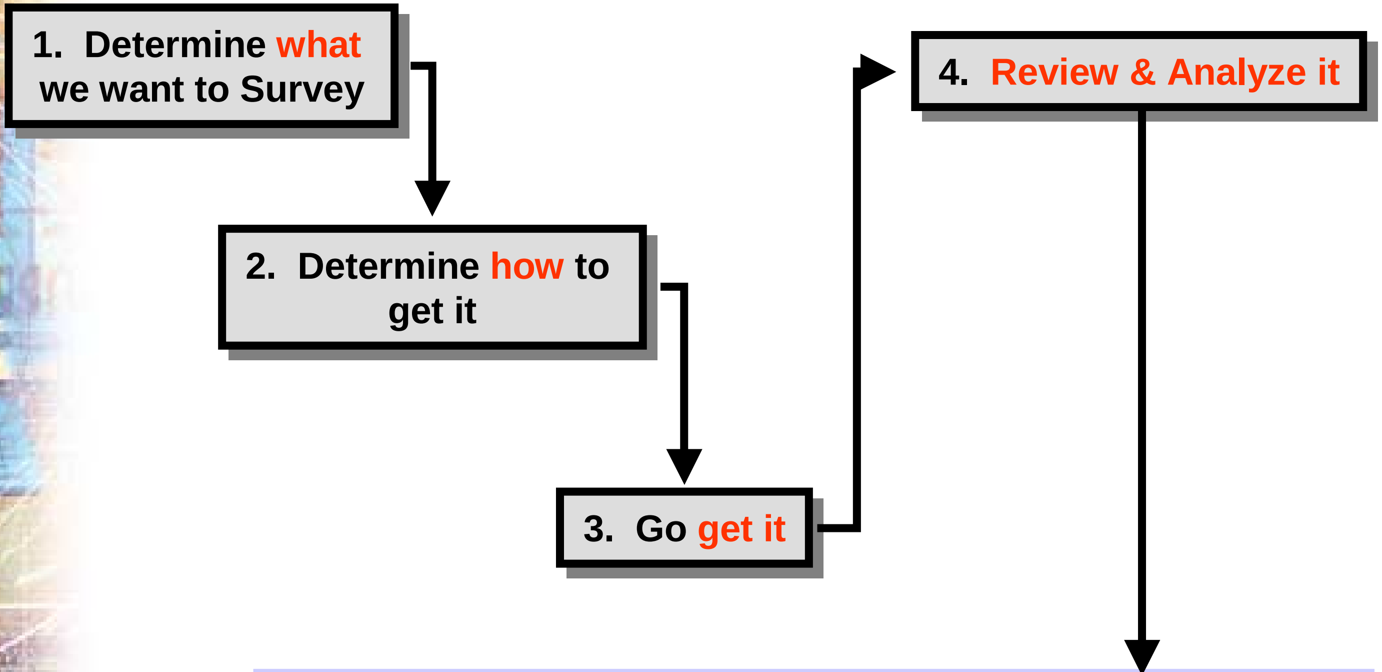
4. Review & Analyze it

- Compile findings
- Bin products into like groupings
- Review groups of products
- Draw conclusions from each group
- Draw overarching conclusions





Approach



1. Determine what we want to Survey

2. Determine how to get it

3. Go get it

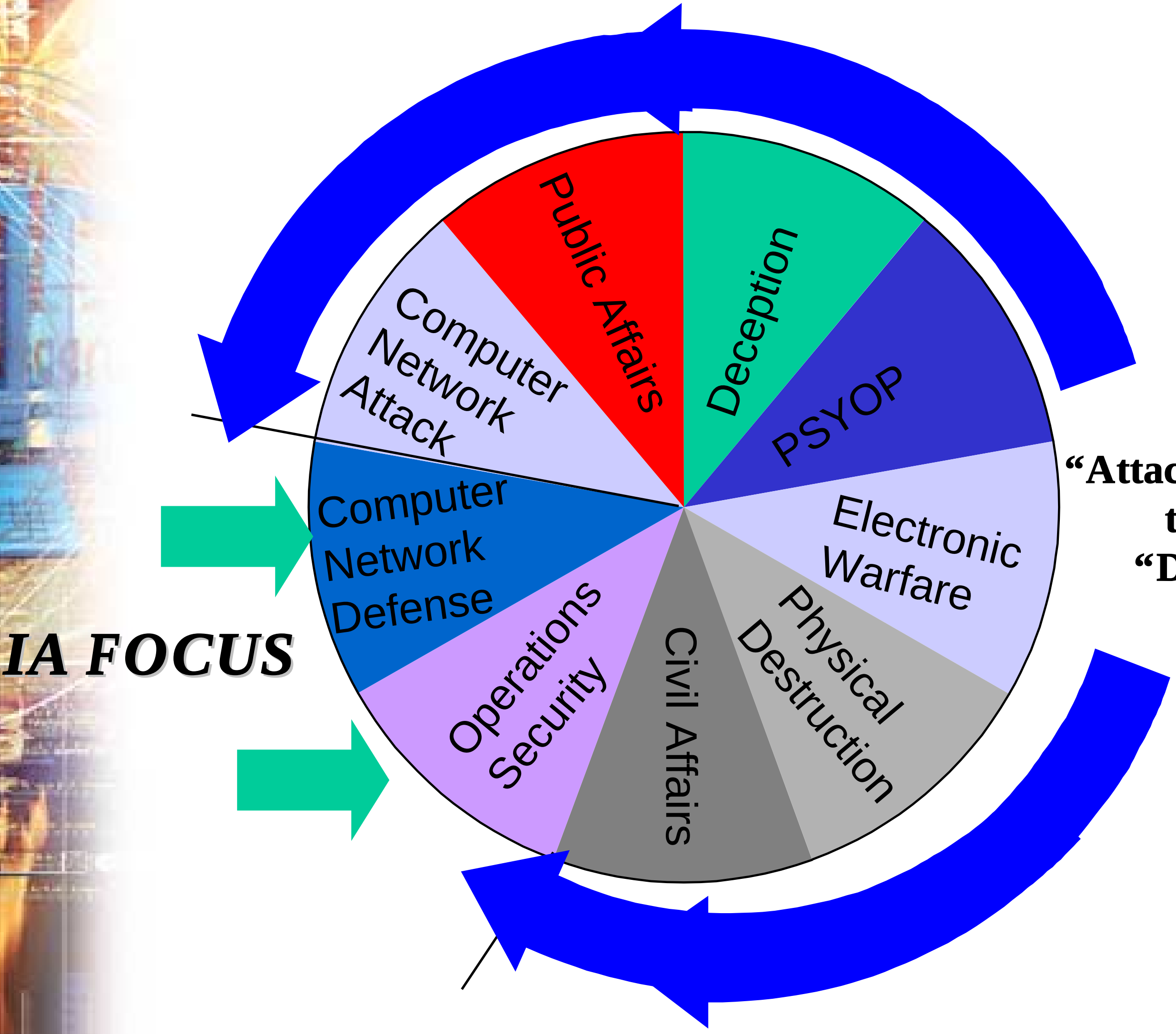
4. Review & Analyze it

- Over 100 organizations were contacted
- 60 unique products/activities were captured, described and categorized

Outline

- Definitions, Objectives, Approach
- **Background**
- Types of IA M&S
- Summary, Conclusions, Needs

The IO "Wheel" Explains Why the Study Looks at IO as well as IA M&S



"Attacks" required to study "Defenses"

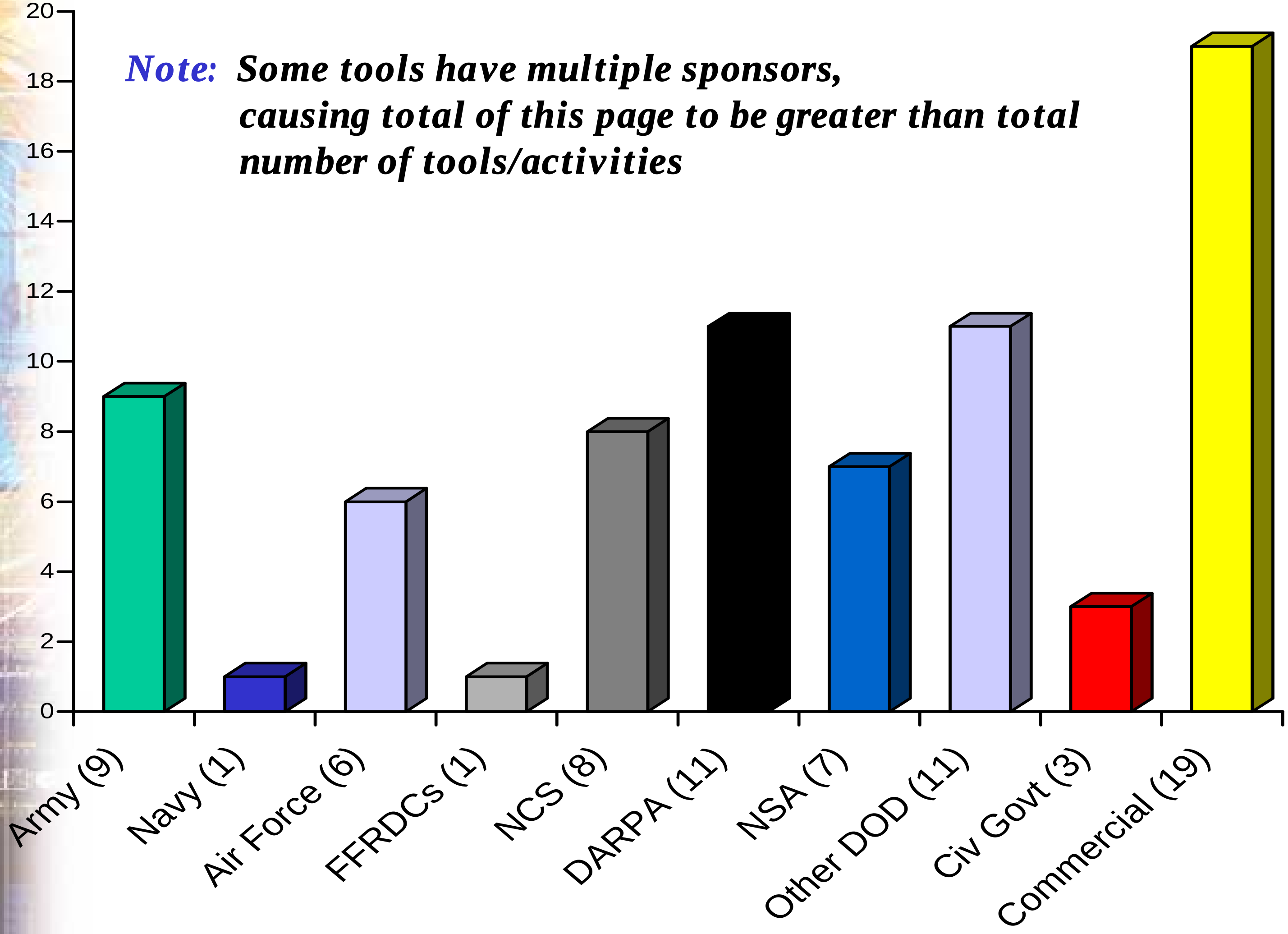
Conclusions from Similar IATAC Report of 1997

- "Future warfighting capabilities depend on IA."
- "Metrics are needed for IA assessments."
- "Additional M&S tools are needed to support IA."
- IA M&S capabilities are nascent."
- One goal of this new report is to understand what progress has been made the past three years

Outline

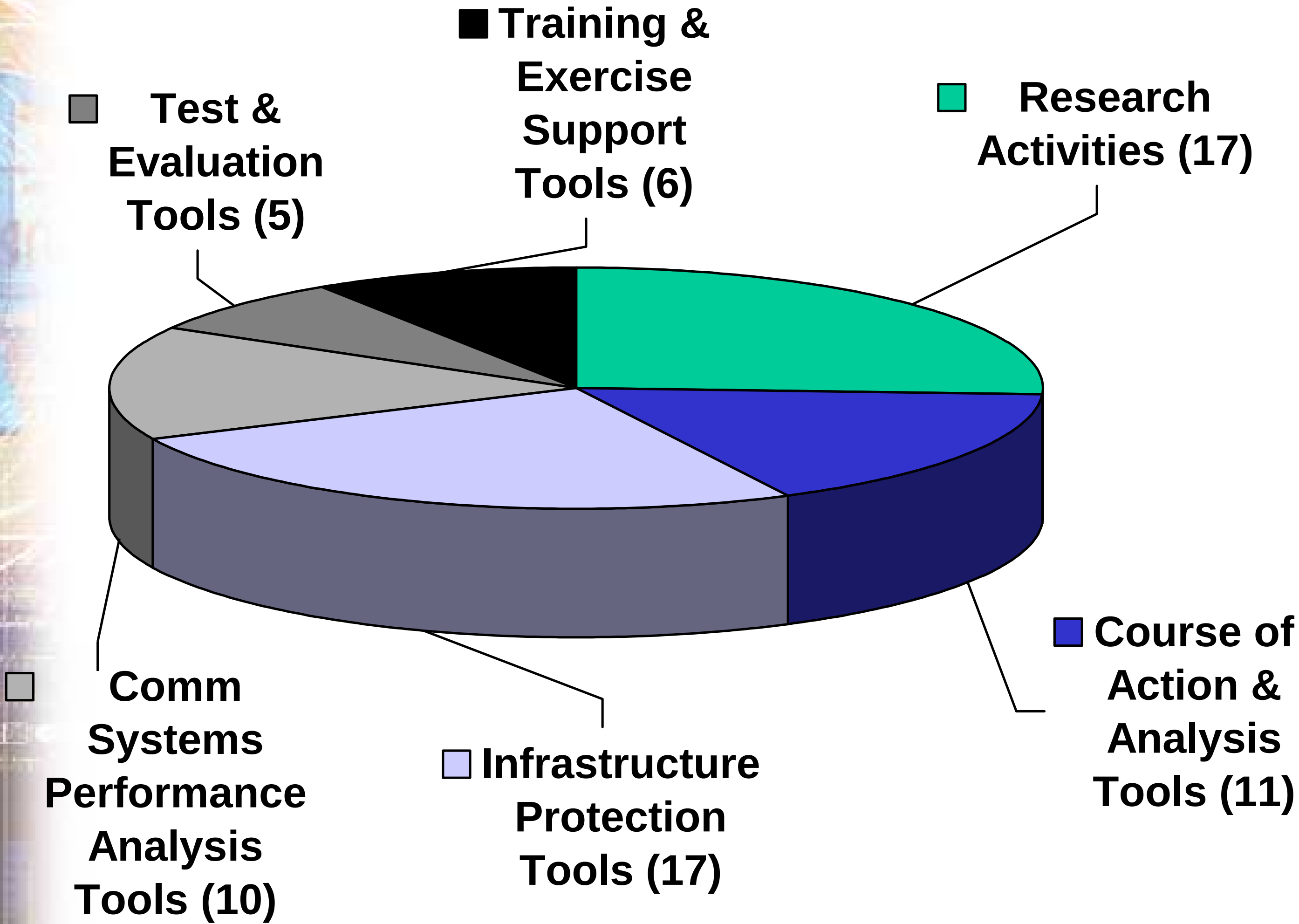
- Definitions, Objectives, Approach
- Background
- Types of IA M&S
- Summary, Conclusions, Needs

Organizations Represented in Report Findings



***Note:* Some tools have multiple sponsors, causing total of this page to be greater than total number of tools/activities**

Six General Areas of IA/IO M&S Activities & Tools


■ Training & Exercise Support Tools (6)
▨ Test & Evaluation Tools (5)
🟩 Research Activities (17)
▨ Comm Systems Performance Analysis Tools (10)
□ Infrastructure Protection Tools (17)
🟦 Course of Action & Analysis Tools (11)

Types of IA M&S (1 of 3)
(Not simulation for simulation’s sake)

- Although some activities seemed to fit into more than one category, all responses were grouped into one of the following:
  - – General research / Body of Knowledge (17)
    - Research and/or databases that support the development of IA M&S tools
  - – Course of Action Planning and Analysis Tools (11)
    - "Providing Warfighters the ability to study and analyze the accomplishment of an operational mission, resulting in a weighted cost/benefit analysis of recommended or preferred options."

Types of IA M&S (2 of 3)

- Infrastructure Protection Tools (17)
  - "Analyzing the ability to defend, safeguard, or shield from injury, loss, or destruction a framework of interdependent networks and systems."
- General Communications Systems Performance Analysis Tools (10)
  - Development environments used to represent the flow of information through a communications infrastructure.

Types of IA M&S (3 of 3)

- Test and Evaluation Tools (5)
  - "Providing a set of stimuli (derived by simulation as opposed to by human intervention) to a specific system under test so as to augment and complement various stages in the material acquisition process.”
- Training and Exercise Support Tools (6)
  - "Providing the proper stimuli to Warfighters to accurately reflect the conditions of an operational mission so as to support a range of training roles, spanning from stand-alone maintenance/operator trainers for individual use, to integrated crew level training systems, to distributed training of Corps and Echelon Above Corps commanders."

Most active area of activity: Infrastructure Protection Tools

Tool	Sponsor	Tool	Sponsor
Authentication, Verification, Integrity Tools and Architecture (AVITA)	Litton PRC	Link Builder	JPO-STC / Booz-Allen & Hamilton
Blitzkrieg System	Future Vision Group	Network Security Simulator (NSS)	Fred Cohen & Associates
Denial of Service Attack Assessment	DARPA	Cyberwar XXI; CRISIS XXI	US Air Force/MITRE/DARPA
D-Wall	Fred Cohen & Associates	SAFEOperations for System Administrators TM	ASD/C3I
EASEL (Emergent Algorithm Simulation Environment and Language)	Carnegie Mellon's Computer Emergency Response Team (CERT) Coordination Center	SimuNet	TeleniX Corporation
HEAT	Sandia National Laboratories	System Administrators Integrated Network Tool (SAINT)	World Wide Digital Security Inc.
INFOSEC Experience-Based Training (IEBT)	Department of Energy / Lawrence Livermore National Laboratory	Tactical Internet Model (TIM)	U.S. Army CECOM
Infrastructure Damage Assessment/ Connectivity Analysis Model (IDA/CAM)	National Communication System / Booz-Allen & Hamilton	Visual Network Rating Methodology	DARPA / National Security Agency (NSA)
Internet Attack Simulator (Maverick)	US Army CECOM / General Dynamics		

Assessment of Infrastructure Protection Tools

- 17 different tools described
- Market forces likely driving investments in these tools
  - A need to investigate ability to protect networks “off-line” without putting network at risk
- Most IP tools are in the areas of network load susceptibility and optimization, which can respectively predict and counter denial-of-service attacks.
- Need a taxonomy of various types of IP tools and the specific issues each one is best at analyzing.
  - There are so many tools similar at the surface but vastly different that re-use is difficult

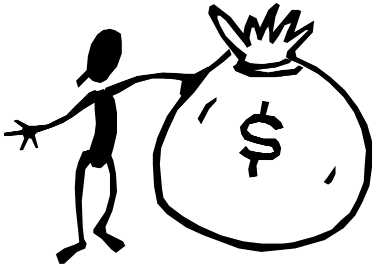
Outline

- Definitions, Objectives, Approach
- Background
- Types of IA M&S
- Summary, Conclusions, Needs

Summary of Findings - The Bright Side

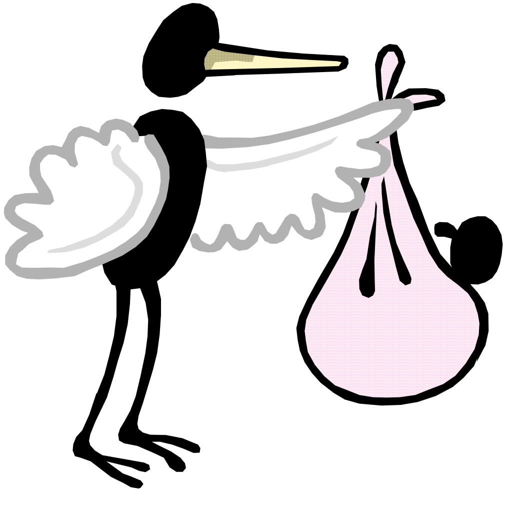
- **Health:**
  - The overall state of IA/IO M&S is quite healthy today, as there are many different M&S tools being used or under development to address a variety of IO and IA-related issues.

- **Funding:**
  - In comparison to the results of a similar IATAC assessment from over three years earlier, many more organizations are now investing in developing M&S tools to address a variety of analytic needs that incorporate some aspect of IA.
- **Visibility:**
  - The need for continued investment in a variety of IA/IO M&S tools is recognized at the highest levels of DoD.



Summary of Findings—The Dark Side

- IA/IO M&S tool development is still very much in its infancy, with much work needed to be done to provide an authoritative body of knowledge to Support future tool developments.
  - It is difficult to accurately model phenomena that we barely understand

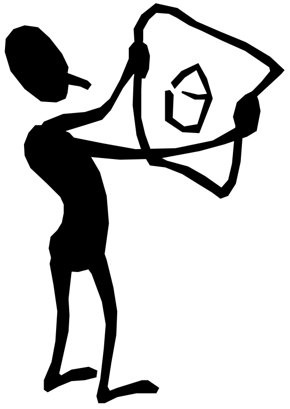


Update of Conclusions from Similar IATAC Report of 1997

- **"Future warfighting capabilities depend on IA."**
  - ***There has been considerable growth in the number and diversity of IA M&S tools at the unclassified level to address a variety of needs.***
- **"Metrics are needed for IA assessments."**
  - ***There has been considerable progress made in developing various bodies of metrics to assist with IA assessments, though there is still a general lack of authoritative and complete data sources.***
- **"Additional M&S tools are needed to support IA."**
  - ***There have been numerous IA/IO course of action tools developed over the past few years to support prioritization and allocation decisions at varying levels of command and various levels of detail.***
- **“IA M&S capabilities are nascent."**
  - ***Considerable progress has been made. The assessment indicates that despite this progress, it seems the community has only begun to scratch the surface of what is needed to provide a robust set of M&S tools.***

Conclusions— IA/IO Body of Knowledge (BOK)

- Much good work has been done in the last few years to provide the foundation for the development of a BOK associated with IA and IO.
- There appears to be a need for a roadmap to enable assessment of how each of these various efforts contributes to the overall development of the BOK as well as to identify gaps that would be prime targets for future research.



IA/IO M&S Needs (1 of 2)

- A common and agreed IA/IO Body of Knowledge (BOK), concentrating on establishing a lexicon, taxonomy and set of quantitative metrics
- More research into human behavioral modeling to reflect the impact of the operator and/or decision maker involved in IA/IO operations
- Tools that better account for the relative cost versus benefit of IA/IO
- A manner in which to aggregate the detailed IA/IO activities that may occur within a conflict into campaign and/or theater-level effects

IA/IO M&S Needs (2 of 2)

- A central repository for all of the above BOK products and M&S tools
- Development and promotion of standards that incorporate all of the above to facilitate re-use and interoperability of IA/IO M&S tools
- Overall conclusion:
  - For IA/IO M&S is to advance much beyond its current state …
    - there is a clear need for a single organization to spearhead such activities and gain buy-in from the rest of the community.

Modeling & Simulation for Information Assurance State-of-the-Art Report (SOAR) - A Summary

•***Principal Author: Gary L. Waag,*** *IATAC*
Iatac@dtic.mil

•***R. Kenneth Heist,*** *MSIAC*
•***Dr. Jerry M. Feinberg,*** *MSIAC*
Lesley J. Painchaud, *MSIAC*

The full IA M&S SOAR can be obtained from either:
IATAC (url: http://iac.dtic.mil/iatac/) or the
MSIAC (url: http://www.msiac.dmso.mil/)

msiac
MODELING AND SIMULATION
INFORMATION ANALYSIS CENTER